| NODIS Library | Legal Policies(2000s) | Search |

NASA Procedural Requirements

NPR 2810.1A
Effective Date: May 16, 2006
Expiration Date: May 16, 2011

COMPLIANCE IS MANDATORY

Printable Format (PDF)

Request Notification of Change (NASA Only)

Subject: Security of Information Technology

Responsible Office: Office of the Chief Information Officer

| TOC | Preface | Chapter1 | Chapter2 | Chapter3 | Chapter4 | Chapter5 | Chapter6 | Chapter7 | Chapter8 | Chapter9 | Chapter10 | Chapter11 | Chapter12 | Chapter13 | Chapter14 | Chapter15 | Chapter16 | Chapter17 | Chapter18 | Chapter19 | Chapter20 | Chapter21 | AppendixA | AppendixB | ALL |

Chapter 14 - System Certification and Accreditation

14.1 Certification and Accreditation

14.1.1 NASA shall follow NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems, guidance in performing certification and accreditation.

14.1.2 NASA shall use ITS-SOP-0005-B, Procedure for Completing a NASA IT Security Program or System Assessment.

14.1.3 The C&A process is a mandatory FISMA process used to ensure that IT systems have effective security controls that have been implemented, or planned for, commensurate with the potential risks to the information. This process is applicable throughout the system's life cycle, including those systems under development and those already in production.

14.1.4 Certification and accreditation activities shall be performed at least once every three years or following a major change to the system.

14.1.5 The C&A process has four distinct phases: initiation, certification, accreditation, and continuous monitoring. Each of these phases is addressed in every IT system accreditation for both operational systems and systems under development regardless of where the system is in the life cycle process.

14.2 Certification Process

Certification is the comprehensive assessment of the technical and non-technical security features and other safeguards of an IT system and establishes the extent to which a particular design and implementation meets documented security requirements. The certification team, led by a CA, can be an individual, group, or organization.

14.3 Certification Process Requirements

14.3.1 The certification and accreditation process shall apply to all master and subordinate systems.

14.3.2 The certification agent shall:

a. Be responsible for conducting a security certification to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome to meet the system's security requirements.

b. Provide the information system owner during the initiation phase with an independent assessment of the SSP to ensure that the plan has documented a set of security controls that is adequate to meet all applicable security requirements.

c. Provide findings and recommendations to the information system owner, who can take corrective actions and update the SSP.

d Document the unmitigated risks in a security assessment report after corrective actions have been made by the information system owner.

14.3.3 Certification of systems that are categorized at the low security impact level shall:

a. Have a "self assessment" of the security controls conducted by the information system owner utilizing ITS-SOP-0005-B, Procedure for Completing a NASA IT Security Program or System Assessment. The security assessment report shall be reviewed by the Center ITSM and included in the SSP by the information system owner.

b. Result in the development of an Accreditation Package as prepared by the CA (see Section 2.5.3.3 e) including:

(1) A transmittal letter. See NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems, Appendix E, for a sample transmittal letter.

(2) A copy of the approved SSP.

(3) The POA&M.

c. Deliver the Accreditation Package to the cognizant Center CIO, ITSM, and the AO as required.

14.3.4 The certification of systems that are categorized at the high or moderate security impact level shall:

a. Consist of a "self assessment" of the security controls conducted by the information system owner utilizing NASA ITS-SOP-0005-B, Procedure for Completing a NASA IT Security Program or System Assessment, until the NIST SP 800-26 and the Agency independent third-party, approved by OSPP, performs the certification of the system.

The self-assessment is performed prior to tasking with the independent certifier. The security assessment report shall be reviewed by the Center ITSM and included in the SSP by the information system owner.

(1) Between the initiation phase and the certification phase, information system owners of IT systems that require Agency contractor certification shall request that the OSPP conduct a review and spot check to ensure security controls are documented during the preparation phase.

(2) Once the OSPP review is satisfactorily completed, the Agency-approved third party, can initiate the certification phase, which constitutes an independent audit.

b. Result in the development an Accreditation Package including:

(1) A transmittal letter; See NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems, Appendix E, for a sample transmittal letter.

(2) Copy of the approved SSP.

(3) The POA&M.

c. Deliver the Accreditation Package to the cognizant Center CIO, ITSM, and the AO as required.

14.3.5 The information system owner shall be responsible for preparing or updating an existing POA&M documenting the remaining actions needed to meet the security requirements of the system.

14.3.6 All SSP packages, in order to prepare for future recertification, shall include a C&A change log to document:

a. Changes made to the system or its environment.

b. In a Security Impact Analysis report, any impact the change may have on the system.

c. Steps taken to eliminate or mitigate any risks resulting from the change.

d. The impact upon the security accreditation decision.

14.4 Accreditation Process

14.4.1 Accreditation is the formal declaration by an AO that an IT system is compliant with established security requirements and is approved to operate using a prescribed set of safeguards. This decision should be based on the residual risks identified during the risk mitigation process. By accrediting an information system, the AO accepts responsibility for the security of the system and is fully accountable for any adverse impacts to the agency if a breach of security occurs.

14.4.2 The security accreditation package documents the results of the security certification process and provides the AO with the essential information needed to make a credible, risk-based decision on whether or not to authorize operation of the information system. The responsibility of the AO for the security accreditation decision and the signing of the accreditation letter (i.e., the acceptability of risk to NASA) cannot be delegated. The information system owner is responsible for the assembly, compilation, and submission of the security accreditation package.

14.4.3 The accreditation phase consists of the security accreditation decision and the security accreditation documentation. The AO shall make one of three decisions:

a. Full Authorization to Operate is issued for the information system if, after assessing the results of the security certification, the residual risk to NASA's operations or assets is deemed fully acceptable to the NASA AO. The information system is accredited without any significant restrictions or limitations on its operation.

b. Interim Authorization to Operate (IATO) is issued if, after assessing the results of the security certification, the residual risk to NASA's operations or assets is not deemed fully acceptable to the NASA AO, and there is an overarching need to place the information system into operation or continue its operation due to mission necessity. An interim authorization provides a limited authorization to operate the information system under specific terms and conditions and acknowledges greater risk to NASA's operations and assets for a limited period. The information system is not considered accredited during the period of IATO. The IATO will not exceed six months.

c. Denial of Authorization to Operate is issued if, after assessing the results of the security certification, the residual risk to NASA's operations or assets is deemed unacceptable to the NASA AO. The information system is not accredited and will not be placed into operation. For an information system currently in operation, all activity will be halted. Failure to receive ATO or an IATO usually indicates that there are major deficiencies in the security controls of the information system. The NASA AO shall work with the information system owner to revise the POA&M to ensure that proactive measures are taken to correct the security deficiencies.

14.4.4 NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems, Section 3.3, details the process and documentation requirements NASA shall follow for accomplishing the security accreditation process and Section 14.5, Accreditation Process Requirements, below, adds specific NASA requirements.

14.5 Accreditation Process Requirements

14.5.1 Responsibility for the security accreditation decision shall not be delegated. Those authorized to act in a functional position in the primary's absence shall inherit the AO's responsibilities. The AO's role shall be consistent with NPD 1000.3, The NASA Organization. The current role of AOs for master and subordinate systems is documented in Figure 14-1.

If the System is,	Then the Master System Authorizing Official is the	And the Subordinate System Authorizing Official is the
Office Automation of Information Technology (OAIT)	NASA Deputy CIO	Center CIO

Program Unique	Deputy Associate Administrator for the Mission Directorate funding the system	Deputy Associate Administrator for the Mission Directorate funding the system
A Multi-funded system (majority funded by single Mission Directorate)	Deputy Associate Administrator for the Mission Directorate funding the majority of the system	Deputy Associate Administrator for the Mission Directorate funding the majority of the system
A Multi-funded system (no majority Mission Directorate funding)	Appropriate Deputy Center Director Directorate	Deputy Center Director
Institutions and Management's Responsibility	Deputy Assistant Administrator for the Appropriate Functional Area	Center CIO
For the Office of Inspector General	NASA Deputy OIG	NASA Deputy OIG
For Office of Safety and Mission Assurance	Deputy Chief Safety and Mission Assurance Officer	Center CIO
For the Chief Engineer	Deputy Chief Engineer	Center CIO
For the Office of Education	Deputy Assistant Administrator for Education	Center CIO
For Office of the CFO	Deputy CFO	Deputy CFO

Figure 14-1 Authorizing Officials

14.5.2 AOs for master systems shall:

a. Make the security accreditation decisions for their master systems, which establish the IT security posture of the associated subordinate systems. See NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems, Appendix E, for sample accreditation decision letters.

b. Explicitly accept the risk to NASA operations, assets, or individuals based on the implementation of an agreed-upon set of security controls and IT security strategy of the system.

c. Advocate to the NASA CFO and CIO that funding be redirected to implement security controls required for master or subordinate systems to achieve full ATO.

d. Concur or non-concur on the determination of the master system's boundaries, the IT security category, the information type, the initial risk assessment, and the selection of security controls which will be inherited by any subordinate system under the authority of the master system.

e. Make the security accreditation decision and sign the accreditation decision letter accepting risk for NASA.

f. Not delegate the role of AO, but, if required, may delegate other supporting accreditation activities, such as reviewing and verifying documents.

14.5.3 AOs for subordinate systems shall:

a. Make the security accreditation decisions for the subordinate systems, which inherits the IT security posture of the associated master system.

b. Explicitly accept the risk to NASA operations, assets, or individuals based on the implementation of an agreed-upon set of security controls and IT security strategy of the system.

c. If necessary, advocate to the NASA CFO and CIO that funding be redirected to implement security controls required for the subordinate systems to achieve full ATO.

d. Concur or non-concur on the system's boundaries, the IT security category, the information type, the initial risk assessment, and the selection of security controls inherited from the master system. Non-concurrences shall indicate that the system should be aligned with a different master or that a new master system must be created.

e. Make the security accreditation decision and sign the accreditation decision letter accepting risk for NASA.

f. Not delegate the role of AO, but, if required, may delegate other supporting accreditation activities, such as reviewing and verifying documents.

14.5.4 A full ATO shall be granted for only three years after which the system shall undergo another certification and accreditation process. The outcome could be a new ATO or an IATO, extension to the existing ATO, or the requirement to halt operations. Requests for up to a six-month extension of an existing full ATO can be submitted through the Center CIO to the NASA OCIO.

14.5.5 An IATO shall be granted for three months, with one extension allowed for an additional three months. After a maximum of six months operating under an IATO, the system shall halt operations. Requests for extension of the IATO shall be submitted through the NASA OCIO and the Office of the Deputy Administrator.

14.5.6 The NASA SAISO and Center ITSMs shall be prohibited from performing the security accreditation decision.

14.6 Additional Certification and Accreditation References

a. NIST SP 800-26, Security Self-Assessment Guide for Information Technology Systems.

b. NIST SP 800-30, Risk Management Guide for Information Technology System.

c. NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems.

| TOC | Preface | Chapter1 | Chapter2 | Chapter3 | Chapter4 | Chapter5 | Chapter6 | Chapter7 | Chapter8 | Chapter9 | Chapter10 | Chapter11 | Chapter12 | Chapter13 | Chapter14 | Chapter15 | Chapter16 | Chapter17 | Chapter18 | Chapter19 | Chapter20 | Chapter21 | AppendixA | AppendixB | ALL |

| NODIS Library | Legal Policies(2000s) | Search |

DISTRIBUTION:
NODIS